Appendix 2B

Miscellaneous guidelines and instructions

This appendix contains the following attachments:

2.4A	System Safety Program Plan Outline
2.6A	Close Call Process
2.7A	Immediate Response to a Mishap
2.7B	Mishap Investigation Process for Type C, D, and “Close Call” Mishaps
2.7C	Mishap Investigation Checklist
2.7D	OSHA and NASA Mishap Categories

Attachment 2.4A
System safety program plan outline

1. What is a system safety program plan?

An SSPP describes your system safety effort for a project or part of a project. It is part of a formal, disciplined system safety program.

You may tailor your SSPP to your project. It must include the entire life of the project from concept, to operations, to phase-out and disposal.

2. SSPP requirements

An SSPP should follow the guidelines in Appendix F of NPR 8715.3, "NASA General Safety Program Requirements."

Each institutional and flight program may have different requirements for an SSPP. This attachment outlines a generic SSPP. See the system safety requirements for the program that you are working on for more details.

An SSPP must:

a. Describe the scope of the project.

b. Describe any relationships between system safety and other project requirements, tasks, and elements. You should cross-reference these to avoid duplication.

c. List any documents and specifications that your system safety effort will use either as directives or as guidance.

d. Identify system safety engineering requirements, tasks, and responsibilities on an item-by-item basis.

e. Be updated as the project direction or requirements change.

SSPP contents

3. System safety organization

The SSPP must describe:

a. The system safety organization or function. Include charts to show the organizational and functional relationships and lines of communication.

b. The responsibility, authority, and accountability of system safety personnel and other organizations (including contractors and subcontractors) involved in the system safety effort. Assign an organization to be responsible for each task. Identify the authority for resolving all identified hazards. Include the title, address, and telephone number of the System Safety Program Manager.

c. How the system safety organization is staffed for the length of the project. Include labor loading and qualifications of key personnel.

d. The interfaces between the system safety organization and other related disciplines such as engineering, occupational safety and health, reliability, quality assurance, or medical support at all levels of the project (NASA, contractor, and subcontractor).

4. System safety project milestones

The SSPP must:

a. Identify safety milestones. Review the effectiveness of the system safety effort at critical safety checkpoints (e.g., design reviews, self-evaluations, operational readiness reviews, audits, etc.).

b. Schedule safety tasks. Show start and finish dates, report dates, review dates, and labor loading, as they relate to other project milestones.

c. Identify other engineering tasks such as design analyses, tests, or demonstrations that also apply to the system safety program. Include the estimated system safety personnel who will do these tasks as part of this section.

5. System safety and risk management

The SSPP must:

a. List the safety standards and system specifications the project either must follow or will adopt as a requirement. Include any system safety requirements or definitions that aren't covered in JSC documents.

b. Describe how you will coordinate the system safety efforts of different parts of the project. Include charters of any system safety groups and methods to:

- Distribute system safety requirements to action organizations.
- Coordinate and integrate hazard analyses.
- Hold management and engineering reviews.
- Report program status.

c. Describe the procedures for assessing risk. Include:

- Hazard severity categories.
- Mishap probability (or frequency) levels.
- The method for finding risk levels such as a risk matrix.
- The acceptable risk levels for the project.

d. Describe the management controls to make sure the project follows safety requirements. Include the process for making management decisions and the level of management required to accept different levels of risk. Include methods to make management aware of and take action on:

- Critical and catastrophic hazards.
- Corrective actions to hazards.
- Mishaps or malfunctions.
- Variances to safety or program requirements.

6. Hazard analyses

The SSPP must describe how you will do hazards analyses for the project to include:

a. The analysis techniques and format that you will use to identify hazards, their causes, their effects, and recommended corrective actions.

b. What analysis techniques you will use and when you will use them.

c. How you will integrate hazard analyses from different organizations such as contractors and subcontractors.

d. A single closed-loop system for tracking hazards to closure.

7. System safety data

The SSPP must:

a. Describe the approach for researching, distributing, and analyzing historical hazard or mishap data.

b. Identify the data management needs for making risk decisions.

c. Identify the safety-related data that you will reference and how you will keep the data. State how Safety and Mission Assurance may access the data.

8. Safety verification and audits

The plan must describe:

a. The verification and audit requirements and procedures to make sure that the system safety program has been implemented.

b. The procedures to make sure that safety information is available for management and engineering review and analysis.

c. The review procedures to make sure that hazardous tests, and especially tests involving human test subjects, are conducted safely.

Attachment 2.4A
System safety program plan outline
(cont.)

9. Training

Describe techniques and procedures to make sure that engineers, test subjects, technicians, operators, and support (including maintenance) personnel understand the objectives and requirements of the system safety program.

10. Other safety reviews or surveys for your project

List any other reviews or audits that will help you evaluate the safety of your project during design or operation. These reviews may include any of the following:

a. Special surveys for very hazardous systems or for changes to these systems to make sure that risks are properly identified and managed.

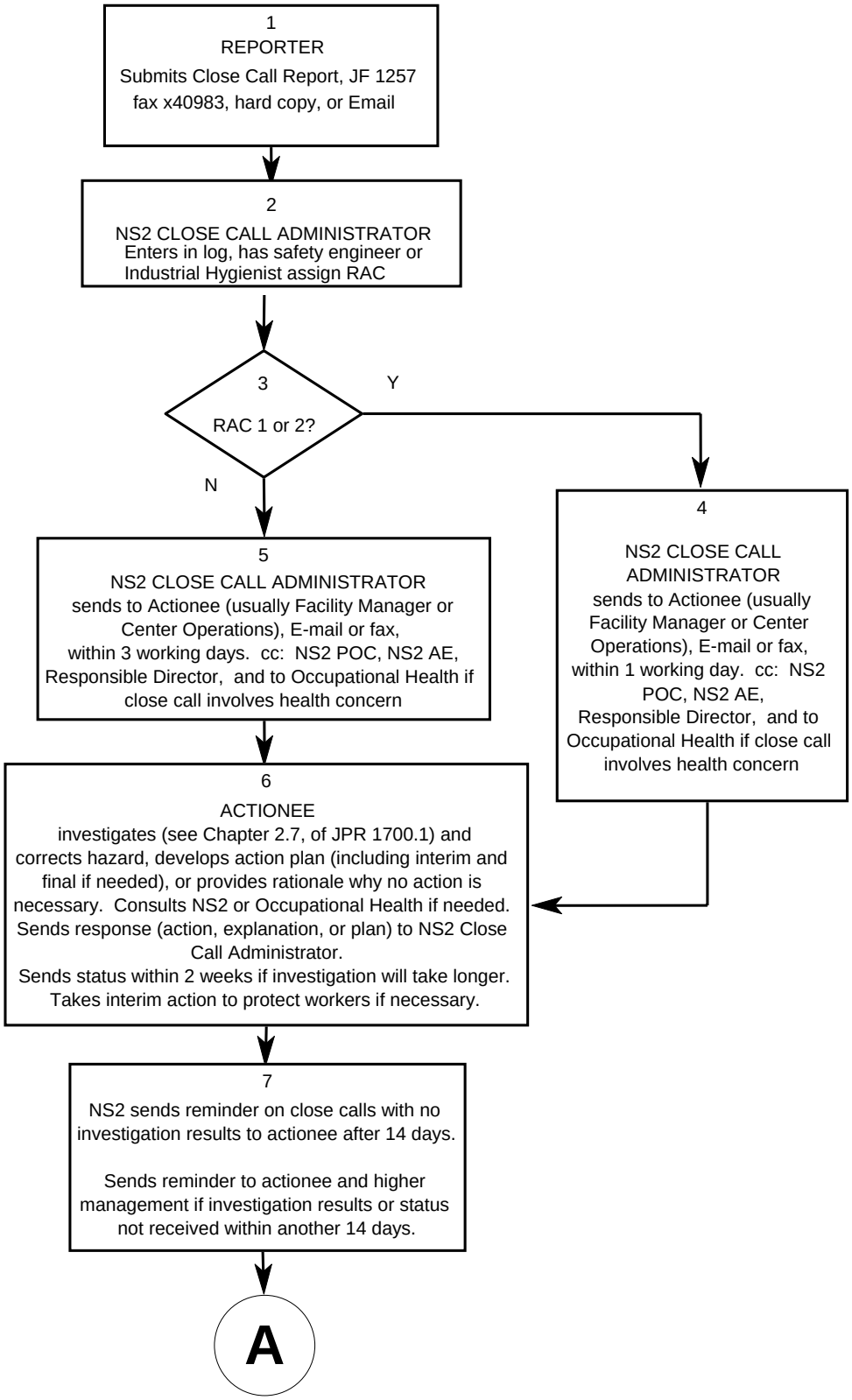
b. A review by experts outside your project during readiness reviews such as TRRs, operational readiness inspections, or acceptance reviews.

c. System safety audits by JSC organizations or NASA Headquarters for major projects and facilities. These audits should be done periodically and consider:

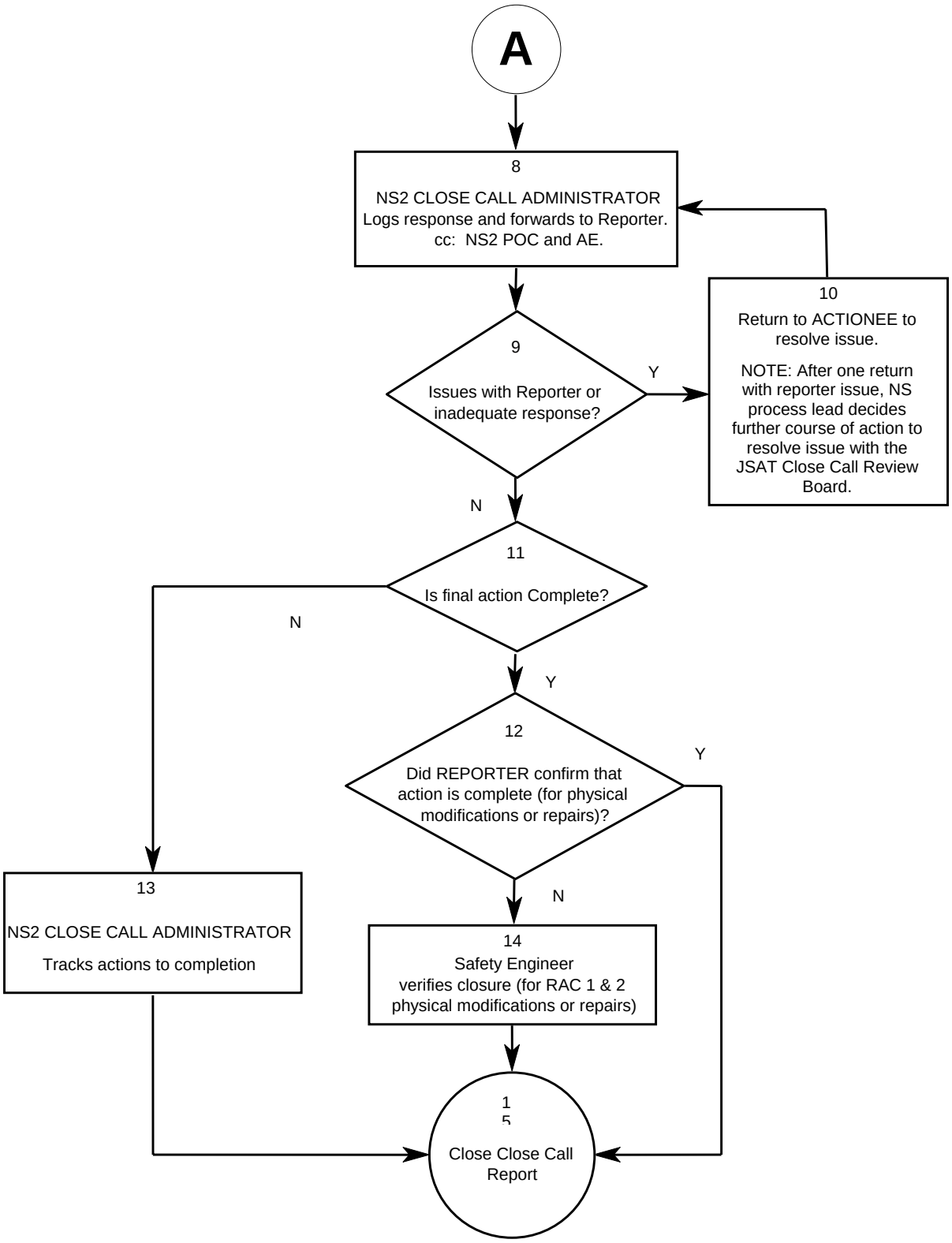
- Did the system perform as planned?
- Were all hazards identified and controlled effectively?
- Did the hazard and risk analysis result in effective risk decisions?
- Have design or operational changes increased the risk of the system?

d. A review by the Operations and Engineering Panel during the detailed design phase as described in paragraph 1.9.3 of NPR 8715.3, "NASA General Safety Program Requirements," for major facilities. The Operations and Engineering Board is a NASA Headquarters panel that reviews certain facilities it chooses to, or is required to, review. You will be notified if the Operations and Engineering Board will review your facility.

Attachment 2.6A
Close call process



Attachment 2.6A
Close Call Process
(continued)



Attachment 2.7A
Immediate response to a mishap

See list of emergency numbers on next page.

If you are on the scene or the first one to arrive:

1. PULL MANUAL FIRE ALARM BOX or DIAL (x33333 at JSC or Sonny Carter Training Facility or x44444 at Ellington Field) for fire, explosion, chemical spills, air emissions (vapor cloud or smoke), personnel rescue, or building evacuation. Give this information to the dispatcher when you telephone:
   - Your name and telephone extension at which you may be called during the emergency
   - Exact location of the emergency
   - Type and extent of emergency

   Stay on the telephone until the dispatcher acknowledges receipt of information.

   If mishap is an on-site vehicle accident, call Security at x34658. If injuries have occurred, call x33333 or x44444 as appropriate.

2. Help the injured only if you can do so without endangering yourself. Never move an injured person unless failure to do so will result in further injury or death. If you can't help or move the injured or ill person, wait for emergency personnel such as the Fire Department or Incident Response Team to arrive.

3. Limit further injury to people, property damage, and impact to the environment as much as possible only if you can do so without endangering yourself.

4. Take ambulatory injured or ill persons to the JSC Clinic, Building 8.

5. Get names and addresses of witnesses.

6. Restrict access to scene and evidence of mishap until investigator arrives or investigation is complete.

7. Notify your supervisor of the emergency and actions taken; request that he or she notify the Safety and Test Operations Division at x32084.

8. In cases of off-site accidents involving NASA property or JSC or contractor personnel:
   - Seek help from nearest medical or fire facility.
   - Follow other appropriate actions such as items 2, 3, 5, 6, and 7 above.

Attachment 2.7A
Immediate Actions After a Mishap
(continued)

Emergency numbers

Dial x33333 (JSC or Sonny Carter Training Facility) or x44444 (Ellington Field) day or night to report:

- Injury – Ambulance
- Fire
- Vehicle accident – Security
- Hazardous materials release or spill – Incident Commander

Other important numbers on site include:

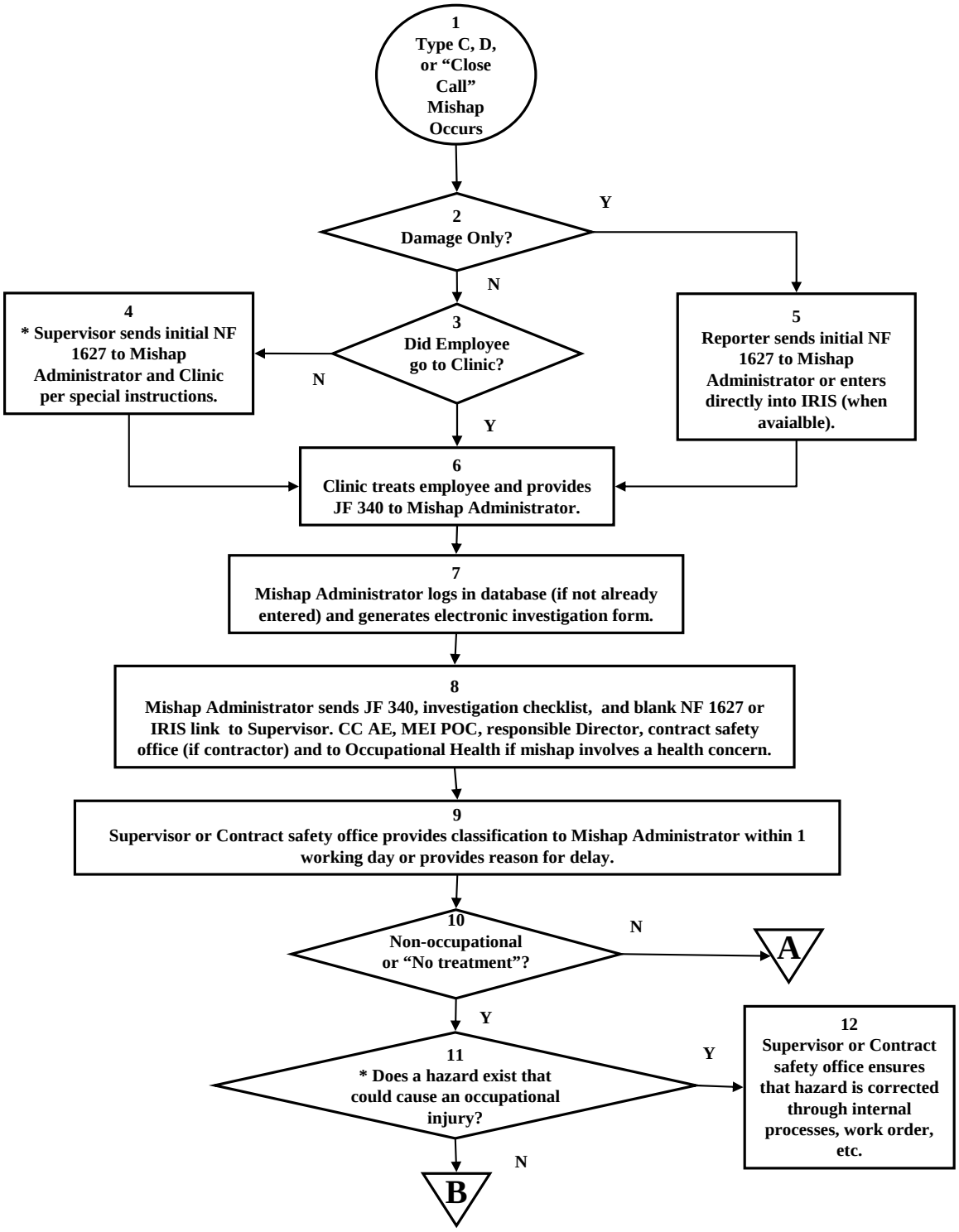
- x34111 – Clinic
- x32038 – Facilities Maintenance and Repairs
- x34317 – Clinic Services Branch
- x36726 – Occupational Health Contractor
- x34900 – Safety and Test Operations Division
- x37084 – Radiological Health Office
- x33061 – Utility interruptions or failure
- x33501 – Environmental Office (daytime only)

Ellington Field, day or night, dial:

- x44444 – Ambulance
- x44444 – Fire
- x33333 – Security

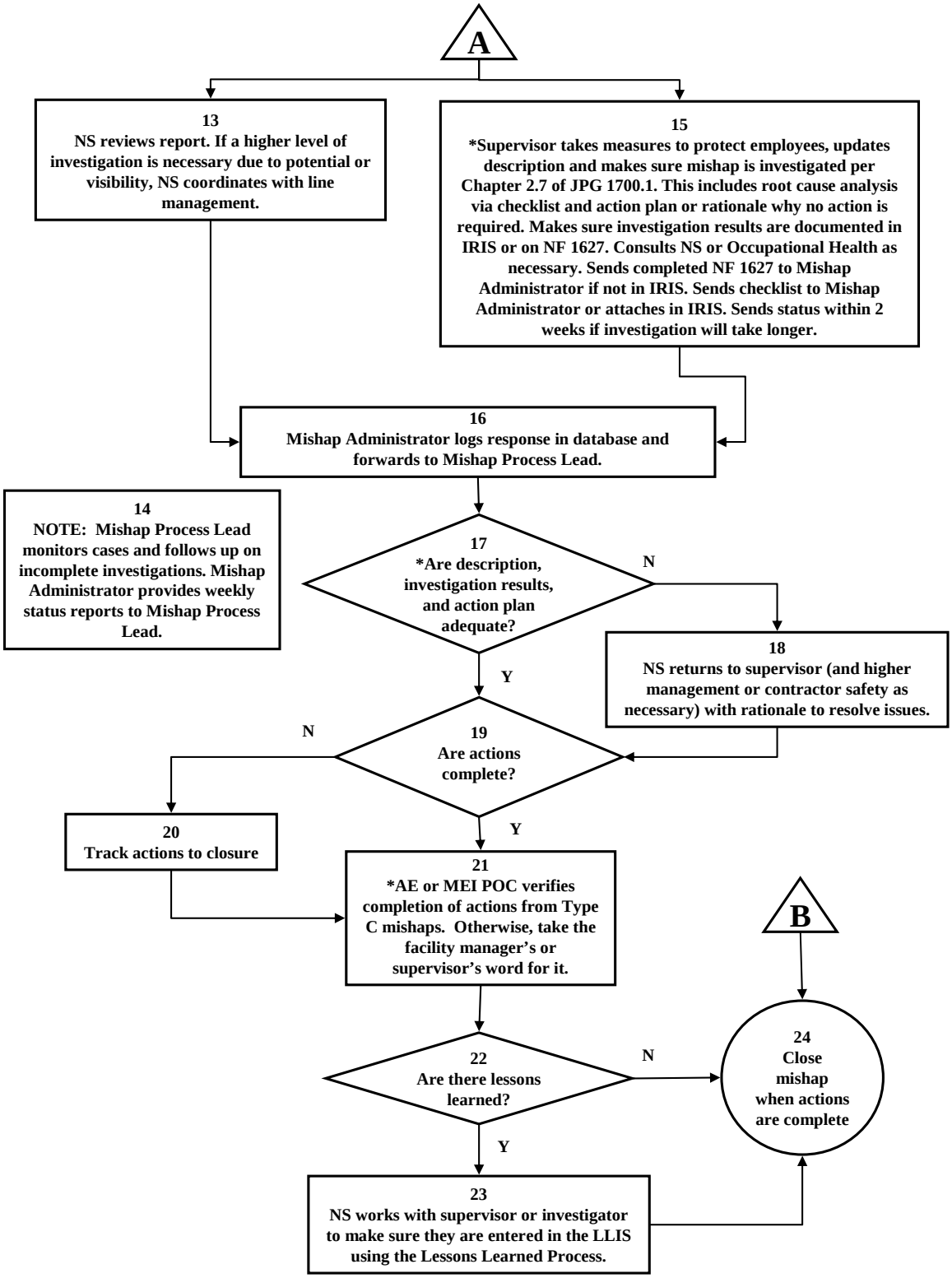
Attachment 2.7B
Mishap Investigation Process for Type C, D, and "Close Call" Mishaps

1.



Verify this is the correct version before you use it by checking the on-line version.

Attachment 2.7B
Mishap Investigation Process for Type C, D, and "Close Call" Mishaps (continued)



Attachment 2.7C

Mishap Investigation Checklist

Complete this checklist by examining the scene, interviewing witnesses, and examining other evidence. Justify "no" answers to questions 1 and 2. Then go to the list of suggested actions.

1.	Were there any unsafe or unhealthful conditions that led to this mishap?	Yes	No
2.	Were there any unsafe acts that led to this mishap?	Yes	No
	If "No," stop here. If "Yes," answer questions 3–9.		
3.	Does a Job Hazard Analysis exist? Yes No		
	a. If so, are the identified hazards adequately controlled?	**Yes**	**No**
4.	Is training necessary for the task?	Yes	No
	a. If so, were employee(s) involved properly trained?	**Yes**	**No**
5.	Are procedures necessary for the task?	Yes	No
	a. If so, do they exist?	**Yes**	**No**
	b. If so, were employee(s) involved aware of them?	**Yes**	**No**
	c. If so, did the employee(s) involved follow them?	**Yes**	**No**
6.	Are safe work practices or requirements necessary for the task?	Yes	No
	a. If so, do they exist?	**Yes**	**No**
	b. If so, are they easy to understand?	**Yes**	**No**
	c. If so, were employee(s) involved aware of them?	**Yes**	**No**
	d. If so, did the employee(s) involved follow them?	**Yes**	**No**
7.	Is PPE necessary for the task?	Yes	No
	a. If so, did employee(s) involved know it is necessary and how to use it properly?	**Yes**	**No**
	b. If so, did employee(s) involved use it properly?	**Yes**	**No**
8.	Are indicators and controls easy to understand and operate?	Yes	No
9.	Are any permits (hazardous operations, confined space, hot work, etc.) required for the task?	Yes	No
	a. If so, were employee(s) involved aware they are necessary?	**Yes**	**No**
	b. If so, were the permits handled properly?	**Yes**	**No**
10.	Were there any other system or management factors that may have contributed to the unsafe act such as:		
	a. Management pressure?	**Yes**	**No**
	b. Inadequate supervision?	**Yes**	**No**
	c. Peer pressure?	**Yes**	**No**
	d. Stress, exhaustion, or workload?	**Yes**	**No**
	e. Boredom or physical discomfort?	**Yes**	**No**
	f. Mismatch of employee to job?	**Yes**	**No**
	g. Off-the-job events that could have affected the mishap?	**Yes**	**No**

Attachment 2.7C
Mishap Investigation Checklist
(continued)

Recommended actions

See the list below for suggested actions. Note actions on investigation form. For incomplete actions, note the responsible person (name, phone, and mail code) and expected completion date.

1. If "Yes," correct the conditions using a work order or internal process.

2. If "Yes," take action as suggested for questions 3–10.

3. If "No," do a Job Hazard Analysis. See URL: http://www6.jsc.nasa.gov/safety/hazard/docs/JSC17773C.doc.
   a. If "No," provide adequate controls for the identified hazards.

4. If "Yes," take action as suggested for 4a below.
   a. Make sure all employees doing this task are properly trained from now on.

5. If "Yes," take action as suggested for 5a–5c below.
   a. If "No," create adequate procedures for the task.
   b. If "No," make sure all employees doing this task are aware of and adequately trained in the procedures.
   c. If "No," determine why the employee(s) failed to follow procedures. If it was an honest mistake, counseling may be in order. If it was a willful disregard for procedures, disciplinary action may be in order.

6. If "Yes," take action as suggested for 6a–6c below.
   a. If "No," create adequate safe work practices or requirements for the task.
   b. If "No," make sure all employees doing this task are aware of and adequately trained in the safe work practices or requirements.
   c. If "No," determine why the employee(s) failed to follow safe work practices or requirements. I f it was an honest mistake, counseling may be in order. If it was a willful disregard, disciplinary action may be in order.

7. If "Yes," take action as suggested for 7a – 7b below.
   a. If "No," make sure all employees doing this task are aware that PPE is necessary and how to use it properly.
   b. If "No," determine why the employee(s) failed to use PPE or use it properly. If it was an honest mistake, counseling may be in order. If it was a willful disregard, disciplinary action may be in order.

Attachment 2.7C
Mishap Investigation Checklist
(continued)

8. If "Yes," take action as suggested for 8a–8b below.
   a. If "No," make sure all employees doing this task are aware that permits are necessary.
   b. If "No," determine why the employee(s) failed to handle the permits properly (or didn't use them). If it was an honest mistake, counseling may be in order. If it was a willful disregard, disciplinary action may be in order.

9. If "No," redesign indicators or controls to make them easier to understand or operate.

10. Were there any other system or management factors that may have contributed to the unsafe act?
    a. If "Yes," identify the source of the management pressure and remove it.
    b. If "Yes," determine what supervision is necessary to do the job safely and make sure it is provided.
    c. If "Yes," identify the source of peer pressure and remove it.
    d. If "Yes," take measures to reduce excess stress, exhaustion, or workloads.
    e. If "Yes," consider automating tasks to prevent boredom or redesign the job to reduce discomfort.
    f. If "Yes," review job qualifications and assignments. Improve employee qualifications or reassign personnel.
    g. If "Yes," be aware of it. Be sensitive to the employee since the circumstances may not have been preventable.

Attachment 2.7D
OSHA and NASA mishap categories

The following table correlates OSHA and NASA definitions.

OSHA Category	NASA category
	Type A Mishap (one or more of the following)
Death or hospitalization of three or more persons for more than observation is immediately reportable to OSHA within 8 hours.	Death A permanent total disability Hospitalization of three or more persons within 30 workdays of the mishap Damage greater than or equal to $1M
Lost workday case involving days away from work (LW-DA).	*Type B Mishap* (one or more of the following) Permanent partial disability Hospitalization of one or two persons within 30 workdays of the mishap Damage greater than or equal to $250,000 and less than $1M
Days away, restricted, transfer (DART) – Cases that involve *days away from work* or *days of restricted work activity*, transfer to another job or any combination of the three. LW-DA – Workdays (consecutive or not) on which the employee would have worked but could not because of an occupational injury or illness, not including the day of the injury. Lost workday case involving restricted duty (restricted work activity) (LW-RD) – Workdays (consecutive or not; not including the day of the injury) on which, because of an injury or illness, the employee: (1) Was temporarily assigned to another job; or (2) Worked at a permanent job less than full time; or (3) Worked at a permanently assigned job but could not do all duties normally connected with that job.	*Type C Mishap* (one or more of the following) Lost workday case Restricted duty Transfer to another job Damage greater than or equal to $25,000 and less than $250,000
No corresponding OSHA category	*Mission or Test Failure* Prevents accomplishing primary mission or test objectives
No corresponding OSHA category	*Environmental Impact* Results in an unplanned and uncontrolled hazardous material spill or rel environmental violation or fine
Medical Treatment Case as defined by OSHA	*Type D* (one or both of the following) Injury or illness without lost time that requires "medical treatment" as d OSHA Damage greater than or equal to $1,000 and less than $25,000
First-Aid Case as defined by OSHA Not OSHA-Recordable	*First-Aid Case* Injury or illness that requires only first-aid treatment
No corresponding OSHA category	*Close Call* (one or both of the following) event or a condition that could have resulted in an injury, an illness, or a erruption of work or environmental spill, release, noncompliance, or nconformance, but did not. Damage less than $1,000

Attachment 2.7C
Mishap Investigation Checklist
(continued)